4Н

УДК 681.215

Я.М. Николайчук
Інститут проблемно-орієнтованих комп'ютерних систем, м. Тернопіль, Україна
ozm@yandex.ru

Теорія цифрових перетворень мультибазисного супершвидкодіючого процесора

Викладені теоретичні основи систем числення та цифрових перетворень у різних теоретико-числових базисах. Розроблена структура супершвидкодіючих мультибазисних процесорів.

Вступ

Світовий досвід створення процесорів для комп'ютерних систем за останні 50 років, поряд із застосуванням теоретико-числового базису (ТЧБ) Радемахера, який породжує двійкову систему числення, демонструє тенденцію все ширшого застосування інших ТЧБ, в тому числі: унітарного, Хаара, Крейга, Крестенсона, Уолша та Галуа. Реалізація спеціалізованих, сигнальних, комутаційних та проблемно-орієнтованих процесорів цифрової обробки даних часто виконується на базі сумісного використання комбінацій названих ТЧБ, наприклад Уолша – Хаара, Крестенсона – Галуа та ін.

Перспективним напрямком розвитку теорії та технологій побудови універсальних комп'ютерних засобів є реалізація супершвидкодіючих мультибазисних RCG-процесорів на основі базисів Радемахера, Крестенсона і Галуа. Відомі успішні спроби розвитку теорії та техніки побудови матричних процесорів на основі двовимірних базисів Радемахера та Галуа, а також конвеєрних спецпроцесорів у базисі Галуа.

Спостережувані тенденції розвитку теорії методології та техніки процесорів комп'ютерних систем обумовлені теоретичним та ідейним насиченням можливостей застосування базису Радемахера для побудови арифметико-логічних компонентів процесорів, до яких ставляться все жорсткіші вимоги щодо швидкодії, покращення регулярності структури та розширення функціональних можливостей.

У зв'язку з цим існує проблема глобального дослідження характеристик «нерадемахівських» ТЧБ та граничних можливостей їх застосування для реалізації компонентів як спеціалізованих, так і універсальних процесорів. При цьому перспективним використанням, крім найбільш сьогодні масового одновимірного (векторного) представлення чисел та виконання арифметико-логічних операцій у базисі Радемахера, є застосування двовимірних систем числення, вертикальної інформаційної технології у базисі Галуа та різних форм багатовимірного представлення чисел у вигляді залишків різних форм системи залишкових класів базису Крестенсона.

1. Теоретико-числові базиси та їх характеристики

Далі приведені кодові матриці відомих ТЧБ, а в табл. 1 їх характеристики у вигляді оцінок сумарного числа елементів відповідних кодових матриць та числа активних елементів.

$$M_{Uni} = \begin{vmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 1 & 0 & \ldots & 0 & 0 \\ 1 & 1 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & 1 & \ldots & 1 & 0 \\ 1 & 1 & 1 & \ldots & 1 & 1 \end{vmatrix} \quad M_{har} = \begin{vmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{vmatrix} \quad M_{LibCr} = \begin{vmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 1 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & 1 & \ldots & 1 & 0 \\ 1 & 1 & 1 & \ldots & 1 & 1 \\ 0 & 1 & 1 & \ldots & 1 & 1 \\ 0 & 0 & 1 & \ldots & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{vmatrix} \quad M_{Wal} = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 1 & 1 & 1 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 1 & 0 & 1 & 0 & 1 \end{vmatrix}$$

$$M_{Gr} = \begin{vmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & 1 & \ldots & 1 & 1 & 1 \\ 1 & 1 & 1 & \ldots & 1 & 1 & 0 \\ 1 & 1 & 1 & \ldots & 0 & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 0 & 0 & \ldots & 0 & 0 & 0 \end{vmatrix} \quad M_{Rad} = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 1 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & 1 & \ldots & 1 & 0 \\ 1 & 1 & 1 & \ldots & 1 & 1 \end{vmatrix} \quad M_{Cres} = \begin{vmatrix} P_1 & P_2 & \ldots & P_n \\ 0 & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 1 \\ 2 & 2 & \ldots & 2 \\ 0 & 3 & \ldots & 3 \\ 1 & 4 & \ldots & 4 \\ 2 & 0 & \ldots & 5 \\ 0 & 1 & \ldots & 6 \\ \ldots & \ldots & \ldots & \ldots \\ a_1 & a_2 & \ldots & a_n \end{vmatrix} \quad M_{Gal} = \begin{vmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{vmatrix}$$

Таблиця 1

Базис	Коди	N	V
Унітарний	Унітарні	N = n	$V = n^2$
Хаара	Розрядно-позиційні	N = n	$V = n^2$
Крейга	Лібова – Крейга	N = 2·n	$V = \frac{N^2}{2}$
Радемахера	Двійкові	N = 2n	$V = N \cdot \log_2 N$
Радемахера	Грея	N = 2n	$V = N \cdot \log_2 N$
Радемахера	Уолша	N = 2n	$V = N \cdot \log_2 N$
Крестенсона	СЗК	$N = \prod_{i=1}^{m} P_i$	$V = \sum_{i=1}^{m} \log_2 (P_i)$
Галуа	М-послідовності	N = 2n – 1	V = N
Галуа	Галуа	N = 2n	V = N

Дані названих таблиць свідчать про те, що однаковими кодовими матрицями володіють базиси Уолша, Грея, Радемахера та Крестенсона, а найбільш компактною матрицею, яка вироджується у вектор, володіє базис Галуа.

2. Системи числення, які породжуються ТЧБ

Фундаментальні теоретичні дослідження ТЧБ показують, що тільки в базисах Уолша та Грея не породжені доступні для практики системи числення, а системи числення, породжені іншими базисами, знайшли широке застосування в теорії та техніці побудови процесорів різних рівнів комп’ютерних систем.

Унітарна система числення, незважаючи на значну інформаційну надлишковість, знайшла успішне застосування в унітарних кореляційних процесорах та в галузі цифрової обробки зображень, особливо опто-електронними процесорами, цифровій голографії, томографії, а також широкого спектру формувачів та перетворювачів форм інформації на рівні сенсорів, мікроконтролерів та телекомунікаційних процесорів.

Система числення базису Хаара знайшла виключно масове застосування в стандартних засобах взаємодії оператор – дисплей, виборчих бюлетневих системах, лото, тестах. Модифікації системи числення базису Хаара широко використані для захисту даних від помилок, наприклад, одновимірних та двовимірних кодах парності та ін.

Система числення базису Крейга знайшла застосування для реалізації найбільш швидкодіючих операційних пристроїв на базі лічильників Джонсона.

Система числення базису Радемахера, виключно її модифікація – двійкова система числення, знайшла на сьогодні найширше застосування для побудови універсальних мікропроцесорів комп'ютерних систем. Значно вужче досягнуто застосування двійково-десяткової, трійкової, двійково-вісімкової, мінус-двійкової та інших її модифікацій.

Система числення залишкових класів (СЗК) базису Крестенсона, розроблена І.Я. Акушським та Д.І. Юдицьким, особливо її цілочисельна форма, широко використовувалась починаючи з 70-х років минулого століття для побудови швидкодіючих спеціалізованих процесорів систем повітряної оборони колишнього Радянського Союзу, а також за той же період реалізована автором у системі контролю та управління процесами буріння «АТОС-Б» та інших цифрових пристроях низових рівнів комп'ютерних систем.

Відомі модифікації СЗК над комплексними числами академіка Р.А. Амербаєва не були масово реалізовані у промислових системах.

Нормалізована форма СЗК, запропонована нами, використана тільки в телекомунікаційних процесорах інформаційних систем нафтогазової промисловості.

Перспективними модифікаціями СЗК, які в даний час глибоко досліджуються на кафедрі спеціалізованих комп'ютерних систем Тернопільського національного економічного університету науковою школою автора, є розроблена досконала цілочисельна та особливо її нормалізована форма, а також запропонована розмежована форма СЗК.

Система числення в базисі Галуа знайшла потужне застосування при реалізації вертикальної інформаційної технології у розподілених комп'ютерних системах контролю та обліку витрати енергоносіїв «ALFIYA», а також реалізації швидкодіючих конвеєрних спецпроцесорів.

В даний час виконуються активні дослідження двовимірних (матричних) форм систем числення базисів Радемахера та Галуа.

Особливий інтерес в світі отримали дослідження багаторівневих форм системи числення базису Галуа, наприклад, по mod 4, що відповідає четвірці нуклеотидів амінокислот A, T, G, C і може бути фундаментальною теоретичною основою інформаційної теорії молекули ДНК, яка характеризується багатьма подібними ознаками з рекурентними послідовностями (ланцюгами) Галуа.

Ще чекає своїх фундаментальних досліджень циліндрична форма кодів двійкової та четвіркової систем числення Галуа. Перспективу ефективного застосування мають коди Галуа для захисту інформації, стиснення даних та реалізації багаторівневих рекурентних структур баз даних.

3. Структура супершвидкодіючих мультибазисних процесорів

На рис. 1 показана структура мультибазисного RCG-процесора із зірково-магістральною архітектурою.

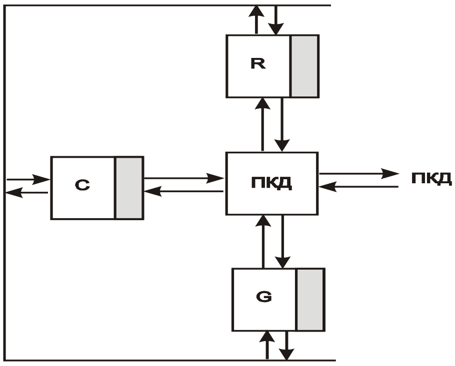


Рисунок 1 – Структура RCG-процесора:
R – процесор Радемахера; C – процесор Крестенсона; G – процесор Галуа;
ПКД – асоціативна пам’ять колективного доступу у базисі Галуа

Дана структура використана в якості високопродуктивного комутаційного процесора системи «Оптіма телеком» і, як показано Н.Д. Круцкевичем, характеризується максимальною емерджентністю і забезпечує підвищення швидкодії обробки даних на 1 – 2 порядки відносно до існуючих процесорів у базисі Радемахера.

Особливістю реалізації пам’яті арифметичного пристрою RCG-процесора є її виконання на основі використання базису Крестенсона – Галуа, що суттєво зменшило об’єм та структурну складність мікроелектронного обладнання.

4. Теорія цифрових перетворень у базисі Крестенсона

4.1. Теоретичні основи цілочисельної форми системи залишкових класів

В основу цілочисельного перетворення СЗК покладена Китайська теорема про залишки [1]. Суть прямого перетворення цілочисельної форми СЗК полягає в тому, що згідно з теоремою про залишки будь-яке ціле число можна однозначно перетворити набором найменших невід’ємних залишків в системі взаємопростих модулів, що відповідає рішенню діафантового рівняння $N_k = b_i (\mod p_i)$, яке відповідає цілочисельному рішенню лінійного рівняння:

$$N_k = a_i p_i + b_i ,$$

де a_i – ранг, b_i – найменший невід’ємний залишок.

При цьому діапазон кодування чисел N_k дорівнює:

$$P = \prod_{i=1}^{k} p_i \text{ ; } 0 \le N_k \le P .$$

Таким чином ціле число N_k однозначно представляється набором залишків b_i.

Зворотне перетворення цілочисельної форми СЗК виконується згідно з аналітичним виразом [2]

$$N_k = res \sum_{i=1}^{k} b_i \cdot B_i (\mod P) , \tag{1}$$

де B_i – базисні числа СЗК, які обчислюються згідно з діафантовим рівнянням:

$$B_i = \frac{P}{p_i} \cdot m_i \equiv 1(\text{mod } P_i). \quad (2)$$

Теорія виконання алгоритму операцій додавання, віднімання та множення в цілочисельній формі СЗК детально викладена в роботах [2], [3]. В основу арифметики залишкових класів покладено глибоке розпаралелювання обробки даних, яке виконується по кожному модулю p_i окремо з виключенням міжрозрядних переносів.

Недоліком цілочисельної форми перетворення СЗК є практична відсутність простої операції порівняння чисел, що суттєво ускладнює реалізації алгоритмів та відповідних процесів ділення. В той же час переваги однотактного матричного виконання інших арифметичних операцій забезпечують широкі перспективи застосування теоретичних основ цілочисельного перетворення СЗК для створення та широкомасштабного впровадження супершвидкісних процесорів в комп'ютерних мережах.

4.2. Теорія нормалізованої форми СЗК

Теоретичною основою утворення нормалізованої форми СЗК (НСЗК) є нормалізація по модулю P обох частин рівняння зворотнього перетворення цілочисельної форми СЗК (1):

$$\frac{N_k}{P} = res\sum_{i=1}^{k}\frac{b_i \cdot B_i(\text{mod } P)}{P},$$

звідки

$$[N_k]_0 = res\sum_{i=1}^{k} b_i \cdot \frac{B_i}{P}(\text{mod } 1),$$

де $0 \le [N_k]_0 \le P-1$; $\frac{B_i}{P} = \frac{1}{p_i}$,

а з врахуванням виразу (2) отримаємо:

$$[N_k]_0 = res\sum_{i=1}^{k} b_i \cdot \frac{m_i}{p_i}(\text{mod } 1) \text{ або } [N_k]_0 = res\sum_{i=1}^{k}[b_i]_0 \cdot m_i(\text{mod } 1), \quad (3)$$

де $[b_i]_0 = \frac{b_i}{p_i}$, а $0 \le [b_i]_0 \le 1$.

Для забезпечення однозначного кодування даних в НСЗК необхідно виконувати умову:

$$\delta_p \le \frac{1}{P}.$$

Дана формула визначає необхідне число розрядів після коми, у відповідній системі числення при представлені величини 1/P в нормалізованій формі, тобто

$$\frac{1}{p_i} = 0,\overbrace{gggg}^{n_i}\overbrace{gggg}^{\delta_p},$$

де g – цифри у відповідній системі числення, n_i – число розрядів, до яких заокруглюється результат ділення з преведенням до меншого цілого, а δ_p – дробова частина, яка визначає величину похибки δ_p, якою нехтують.

Таким чином аналітичний вираз з НСЗК в СЗК отримує вигляд:

$$N_k = \text{int}[N_k]_0 \cdot P,$$

де int – символ операції виділення цілої частини.

Перевагою НСЗК є виконання операцій над залишками в нормалізованій формі, що спрощує реалізацію процесорів на основі даного базису за рахунок виключення нелінійних операцій отримання залишку по кожному з модулів процесора, а також заміни операції по «mod P» на операцію по «mod1», яка виконується шляхом простого відкидання цілої частини результату згідно з операцією int.

4.3. Теорія досконалої форми СЗК

Аналіз формули перетворення СЗК (1) може бути представлений в наступному вигляді:

$$N_k = res\sum_{i=1}^{k} b_i \cdot \frac{P}{p_i} \cdot m_i (\bmod P), \qquad \text{де } 0 \le m_i \le p_i - 1. \qquad (4)$$

Очевидно, що наявність коефіцієнтів m_i в формулі (4) ускладнює реалізацію алгоритму виконання цілочисельного перетворення СЗК. Дослідження різних наборів p_i, яким відповідають набори коефіцієнтів m_i в теоретико-числовому аспекті показали, що існують такі набори модулів $p_1, p_2, ..., p_k$, які відповідають умовам взаємної простоти з одиничними коефіцієнтами $m_i(m_1 = m_2 = ... = m_i = ... = m_k = ... = 1)$.

Пошук наборів модулів, що породжують ДСЗК, є окремою актуальною задачею фундаментального рівня, яка досліджувалась в роботі [1].

4.4. Аналітика досконалої нормалізованої форми СЗК (НДСЗК)

Для створення повної функціонально-ефективної СЗК потрібно спростити існуючі алгоритми виконання операцій порівняння чисел. Умову створення швидкісного пристрою в РСЗК задовольняють алгоритми обчислення всіх арифметичних операцій, крім ділення. Для реалізації операції ділення потрібна НДСЗК. Теоретичною основою даної форми є рівняння (3), підставивши в яке $m_1 = m_2 = m_k = 1$, отримаємо базове рівняння перетворення НДСЗК у вигляді:

$$[N_k]_0 = res\sum_{i=1}^{k}[b_i]_0 (\bmod 1). \qquad (5)$$

З рівняння (5) видно, що з перетворення НДСЗК виключена операція множення і саме перетворення виконується у вигляді сумування нормалізованих залишків $[b_i]_0$ по mod1, що відповідає операції int відкидання цілої частини результату.

5. Теорія розмежованої форми СЗК

Теоретично основою РСЗК є цілочисельна форма СЗК, рівняння якої представлено у вигляді суми:

$$N_k = N_{1k} + N_{2k} + ... + N_{ik} + ... + N_{nk},$$

де N_{ik} – m-розрядний (розмежований) фрагмент числа N_k, яке представлене у двійковій системі числення, числового базису Радемахера. Наприклад 32-розрядний процесор СЗК може бути розмежований на 4 фрагменти по 8 біт (рис. 2).

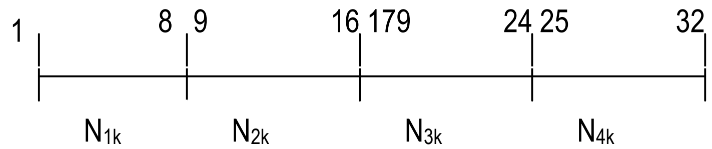


Рисунок 2 – Процес розмежування 32-розрядного процесора

Таким чином, пряме перетворення РСЗК отримає вигляд:

$$b_1 = (b_{11} + b_{21} + ... + b_{r1} + ... + b_{n1}) \bmod p_1$$
$$b_2 = (b_{12} + b_{22} + ... + b_{r2} + ... + b_{n2}) \bmod p_2$$
$$N_k = \quad ... \quad b_i = (b_{1i} + b_{2i} + ... + b_{ri} + ... + b_{ni}) \bmod p_i$$
$$b_k\ b_2 = (b_{1k} + b_{2k} + ... + b_{rk} + ... + b_{nk}) \bmod p_k.$$

При цьому математичні операції над числами в РСЗК можуть бути розмежовані по кожному із фрагментів процесора, що забезпечує ще більш глибокий рівень розпаралелювання обробки інформації, а відповідно підвищення швидкодії процесора СЗК.

Таким чином, у загальному вигляді зворотне перетворення РСЗК аналітично описується виразом: $N_k = res\sum_{r=1}^{n}\sum_{i=1}^{k} res(b_{1i} + b_{2i} + ... + b_{ri} + ... + b_{ni}) \bmod P_i \cdot B_i \bmod P.$

Реалізація процесора на основі даної формули у вигляд РСЗК може бути виконана з суттєвим зменшенням апаратних засобів за кожним з модулів.

6. Теорія перетворень у базисі Галуа

Операція сумування кодів у базисі Галуа для суматорів в діапазоні $2^k - 1$ виконується шляхом виконання логічних операцій над бітами коду Галуа першого з доданків згідно з таблицею логічних рівнянь, що описують другий доданок. В табл. 2.12 подані формули логічного опису бітів другого доданку, на прикладі 4-розрядного коду Галуа для суматорів в діапазоні 2^k, що досягається введенням додаткової комбінації «0000» в позиції 12.

Таблиця 2

Десят-кове значен.	Код Галуа	Формула суматора			
		b_4	b_3	b_2	b_1
0	1111	b_4	b_3	b_2	b_1
1	1110	b_3	b_2	b_1	$b_1 \oplus b_4 \oplus b_3$
2	1101	b_3	b_1	b_2	$b_1 \oplus b_4$
3	1010	b_2	b_2	$b_1 \oplus b_4$	$b_1 \oplus b_2 \oplus b_4$
4	0101	b_1	$b_1 \oplus b_4$	$b_1 \oplus b_2 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3 \oplus b_4$
5	1011	$b_1 \oplus b_4$	$b_1 \oplus b_2 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3$
6	0110	$b_1 \oplus b_2 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3$	$b_2 \oplus b_3 \oplus b_4$
7	1100	$b_1 \oplus b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2 \oplus b_3$	$b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_3$
8	1001	$b_1 \oplus b_2 \oplus b_3$	$b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_3$	$b_2 \oplus b_4$
9	0010	$b_2 \oplus b_3 \oplus b_4$	$b_1 \oplus b_3$	$b_2 \oplus b_4$	$b_1 \oplus b_3 \oplus b_4$
10	0100	$b_1 \oplus b_3$	$b_2 \oplus b_4$	$b_1 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2$
11	1000	$b_2 \oplus b_4$	$b_1 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2$	$b_2 \oplus b_3$
12	0000	$b_1 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2$	$b_2 \oplus b_3$	$b_3 \oplus b_4$
13	0001	$b_1 \oplus b_2$	$b_2 \oplus b_3$	$b_3 \oplus b_4$	b_4
14	0011	$b_2 \oplus b_3$	$b_3 \oplus b_4$	b_4	b_3
15	0111	$b_3 \oplus b_4$	b_4	b_3	b_2

Такий спосіб опису функцій суматора в базисі Галуа передбачає емуляцію його роботи виключно програмним шляхом, що не дозволяє перейти до його апаратної реалізації. В роботі запропоновано метод виконання операції сумування на основі матриці коефіцієнтів d_{ij} (табл. 2.13), яка використовується для логічного формування бітів коду Галуа суми доданків згідно з виразом:

$$b_i = d_{i,k} \cdot b_k \oplus d_{i,k-1} \cdot b_{k-1} \oplus ... \oplus d_{i,1} \cdot b_1 .$$

Таблиця 3

Десяткове значення	Код Галуа	Формула суматора			
		d_{j4}	d_{j3}	d_{j2}	d_{j1}
0	1111	1000	0100	0010	0001
1	1110	0100	0010	0001	1001
2	1101	0010	0001	1001	1011
3	1010	0001	1001	1011	1111
4	0101	1001	1011	1111	0111
5	1011	1011	1111	0111	1110
6	0110	1111	0111	1110	0101
7	1100	0111	1110	0101	1010
8	1001	1110	0101	1010	1101
9	0010	0101	1010	1101	0011
10	0100	1010	1101	0011	0110
11	1000	1101	0011	0110	1100
12	0000	0011	0110	1100	1000
13	0001	0110	1100	1000	0100
14	0011	1100	1000	0100	0010
15	0111	0111	1110	1101	0011

Розглянемо приклад виконання операції додавання двох чисел в базисі Галуа на основі матриці коефіцієнтів d_{ij}. Нехай $X_{(10)} = 2$; $Y_{(10)} = 5$, тоді $X_G = 1101$; $Y_G = 1011$. Тобто X_G відповідає коду $b_4 = 1$; $b_3 = 1$; $b_2 = 0$; $b_1 = 1$, а код Y_G згідно з табл. 2.13 відповідає логічним операціям над бітами X_G: $b_1 \oplus b_2 \oplus b_4 ; b_1 \oplus b_2 \oplus b_3 \oplus b_4 ; b_1 \oplus b_2 \oplus b_3 ; b_2 \oplus b_3 \oplus b_4$, що відповідає кодам d_{ij} 1011; 1111; 0111; 1110 з табл. 2.14. Тобто результат сумування даних чисел виконується за допомогою логічної обробки кодів X_G та коефіцієнтів d_{ij}, які відповідають коду Y_G:

$$G_4 = 1 \wedge b_4 \oplus 0 \wedge b_3 \oplus 1 \wedge b_2 \oplus 1 \wedge b_1 = 1 \wedge 1 \oplus 0 \wedge 1 \oplus 1 \wedge 0 \oplus 1 \wedge 1 = 1 ;$$

$$G_3 = 1 \wedge b_4 \oplus 1 \wedge b_3 \oplus 1 \wedge b_2 \oplus 1 \wedge b_1 = 1 \wedge 1 \oplus 1 \wedge 1 \oplus 1 \wedge 0 \oplus 1 \wedge 1 = 1 ;$$

$$G_2 = 0 \wedge b_4 \oplus 1 \wedge b_3 \oplus 1 \wedge b_2 \oplus 1 \wedge b_1 = 0 \wedge 1 \oplus 1 \wedge 1 \oplus 1 \wedge 0 \oplus 1 \wedge 1 = 0 ;$$

$$G_1 = 1 \wedge b_4 \oplus 1 \wedge b_3 \oplus 1 \wedge b_2 \oplus 0 \wedge b_1 = 1 \wedge 1 \oplus 1 \wedge 1 \oplus 1 \wedge 0 \oplus 0 \wedge 1 = 0 .$$

Отримана система логічних рівнянь дозволяє синтезувати структуру 4-бітового суматора Галуа.

Висновки

В даній роботі викладені основні теоретичні засади побудови супершвидкодіючих мультибазисних процесорів, які обґрунтовують перспективний напрям розвитку супершвидкодіючих мультибазисних процесорів, в першу чергу спеціалізованого, а в майбутньому ефективного універсального застосування.

Література

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных класах. – М: Сов. радио, 1968. – 440 с.
2. Николайчук Я.М., Волинський О.І., Кулина С.В. Теоретичні основи побудови спецпроцесорів у базисі Крестенсона // Вісник Хмельницького національного університету – 2007. – Т.1(93), №3. – С. 85-90.
3. Бухштаб А.А.Теория чисел. – М.: Просвещение, 1966. – 384 с.

Стаття надійшла до редакції 29.07.2008.